Education International
Internationale de l'Education
Internacional de la Educación

http://www.ei-ie.org

5, Bd du Roi Albert II, 9th
1210 Brussels, Belgium
Tel +32 2 224 06 91/92
Fax +32 2 224 06 94
secretariat@csee-etuce.org
http://www.csee-etuce.org

ETUCE
European Trade Union Committee for Education
EI European Region

ETUCE's guidelines on the new EU General Data Protection Regulation (GDPR)

Adopted by the ETUCE Bureau on 29 May 2018

The new General Data Protection Regulation (GDPR) comes into force on 25 May 2018 at national level. This will have an impact on students', teachers' and union members' data protection and privacy - as mentioned in the ETUCE statement on the EU Digital Education Action Plan 2020.

ETUCE general views to the new GDPR:

Data protection, privacy and online security in schools and in trade unions is fundamental. Teachers, schools and trade unionists should regard the introduction of the GDPR regulation as a way of further enhancing how they deal with personal data. New GDPR rules should respect existing data protection systems and only complement them for a more effective protection when required.

Indeed, the adaption to the GDPR entails an administrative and technical burden; teachers and their unions should be involved in the implementation of the GDPR in their country, in particular, to ensure it does not create additional demands and workload on teachers in applying and implementing compliant data protection policies or imply a shift of responsibility to them. Employers in education are responsible for ensuring that education institutions comply with the GDPR and are covered by the necessary public funding, in particular, in terms of purchase, adaptation and implementation of software and hardware for information transferability. Indeed, while the new GDPR regulations mean more accountability, this should not lead to unnecessary costs, tougher penalties and cumbersome requirements to prove evidence compliant with the new data protection standards both in automatic processes and in manual filing systems.

ETUCE guidelines to facilitate compliance with the new GDPR [1] as well as to minimise the risks associated to data protection handling and management in schools and trade unions:

1.- Designate a data controller (e.g. the relevant authority) who has to keep a record of all the processing activities for which the entity is responsible and designate a **data processor** (e.g. school headmaster) to keep a record of all categories of processing activities carried out on behalf of the controller.

2.-Ensure that **t**he data controller and processor comply with their duty of appointing a **data protection officer (DPO)**. In addition, schools and trade unions must ensure that their third party suppliers who may process any of their data is GDPR compliant and must have legally binding contracts with any company that processes any personal data.

3.-The DPO should ensure an **appropriate level of security by technical and organisational measures** such as 'pseudonymization' and encryption of personal data; the ability to ensure

[1] For more information, please consult the GDPR practical guide for trade unionists (March 2018).

confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing; assessing and evaluation the effectiveness of technical and organizational measures for ensuring the security of the processing.

4.-Put in place adequate measures to ensure the **principle of lawful processing** is the core of the new GDPR. It means that personal data must be:
a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) accurate and where necessary :

1. kept up to date (inaccurate personal data must be erased or rectified without delay);
2. storedin a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed;
3. processed in a manner that ensures appropriate security of the personal data.

5.-Develop an approach that allows to comply with the requirement that **consent must be explicitly given** to anything that is not within the normal management of the school, especially if it involves a third party managing the data. Parents (or pupils themselves depending on their age and the case) must express consent for their (child's) data to be used outside of the normal management of the school. Indeed, the data subject must give consent to the processing of his or her personal data for one or more specific purposes, necessary to protect his/her relevant legitimate interest. Consent must be considered as a "free, clear and affirmative act" - e.g. while ticking a box can be an adequate method of consent, pre-ticked boxes cannot. Consent given in a written declaration must be made in "a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language"

6.- Special categories of data (particularly sensitive) include trade union membership and data which reveals an individual's racial or ethnic origin; political opinion, religious or philosophical believes, genetic data and biometric data for the purpose of identifying an individual, data concerning health or data concerning a person's sex life or sexual orientation. Processing is more stringent, in the course of its legitimate activities or trade union aims. In these cases, appropriate safeguards must be put in place and the processing must relate solely to members, former members or members who are regularly in contact with the union and the union purpose. Personal data must not be disclosed outside the union without the consent of data subjects. Explicit consent must be given to process data-.Protecting the vital interest of the data subject and processing is necessary for carrying out obligations and exercising specific rights in the field of employment and social security law.

7.-The DPO has the **duty to provide the information** to individuals when they ask for their personal information and also to facilitate the exercise of the data subject's rights. They include **right of access** (free of charge and at reasonable interval in order to verify the lawfulness of the processing); **right to rectification** (without delay) and **right to be forgotten or right to have data erased without delay** (if the personal data is no longer necessary for the purposes for which it was collected; in case of withdrawal of consent; in case of unlawful processing; in case of no overriding legitimate grounds for processing and if the information was collected by "information society/online services" when he/she was a child).

8.-Put in place measures to ensure other rights of the data subject such as the **right to**

restrict processing by the DPO (in case of objection to the processing, in case of doubts about its accuracy; in case of unlawful processing and the data subject does not want the data to be erased); the **right to data portability** (where there is automated processing based on an individual's consent or performance of a contract, an individual has the right to receive his/her data from the DPO in a structured, commonly used and machine-readable format and is entitled to transmit it to another DPO without hindrance from the first); and the **right to object** to the data processing at any time

9.-In practice, **recommended electronic systems and manual filing systems which help ensure data protection** are:
a) storing paper records in a locked cabinet overnight;
b) keeping papers out of view of visitors;
c) locking away laptops d) ensuring all computers, laptops, and ICT devices are suitably password protected;
e) regularly updating software and anti-virus programmes to prevent loss of data;
f) encrypting documents containing special categories of data such as union membership**;**
g) not relying on regularly using flash drives for teaching or document storage purposes.

10.-At the time of **sending emails** (e.g. to a number of recipients and identifying them as either union members or non-members), it is recommended to use the 'BCC' (blind carbon copy) field in the email to list their addresses, and send it to oneself. That way, your own email will be the only email address that is visible.

11.-Teaching privacy and data protection in schools has become also important in recent years[2]. For teachers to be able to effectively transfer their personal data protection knowledge, and raise the awareness and improve the skills of children and youth in the field of privacy protection, proper educational materials are a key prerequisite. **National data protection authorities (DPAs) should produce those teaching materials in consultation with the education trade unions** taking account of the different school strategies and teachers' training needs in this respect.

[2] Dr Gloria González Fuster and Dr Dariusz Kloza (eds.) "The European Handbook for Teaching Privacy and Data Protection at Schools", 2016, Vrije Universitet Brussel. Law Science Technology & Society (LSTS) EAP.